REMARKS

Claims 1, 5-9, and 11-36 are all the claims presently pending in the application.

While Applicants believe that all of the claims are patentable over the prior art of record, to expedite prosecution, claims 9, 15, 17, and 33 are amended to define more clearly the features of the invention. Claim 9 is amended merely to incorporate the features of claim 10. Claim 10 correspondingly is canceled without prejudice or disclaimer. Claims 31-36 also are amended to overcome the rejection under 35 U.S.C. § 101. No new matter is added.

It is noted that the claim amendments are made only for more particularly pointing out the invention, and not for distinguishing the invention over the prior art, narrowing the claims or for any statutory requirements of patentability. Further, Applicant specifically states that no amendment to any claim herein should be construed as a disclaimer of any interest in or right to an equivalent of any element or feature of the amended claim.

Claims 1, 14-16, 31, and 32 stand rejected under 35 U.S.C. § 101 as allegedly being inoperative and lacking utility.

In a new ground of rejection (which was raised in the Examiner's Answer), Claims 31-36 stand rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter.

Claims 1 and 5-36 previously stood rejected under 35 U.S.C. § 103(a) as being unpatentable over Borza (U.S. Patent No. 6,446,210) in view of Kharon, et al. (U.S. Patent No. 6,487,662; hereinafter "Kharon"). However, in the Examiner Answer the rejection under 35 U.S.C. § 103 was revised such that Claims 1, 5-8, 10-14, 16, 18-26, 28-32, and 34-36 now are rejected under 35 U.S.C. 103(a) as being unpatentable over Borza in view of Kharon.

In a new ground of rejection (which was raised in the Examiner's Answer), Claims 9, 15, 17, 27, and 33 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Borza (U.S. Patent No. 6,446,210).

These rejections are respectfully traversed in the following discussion.

I. THE CLAIMED INVENTION

The claimed invention provides a method and system of processing semiotic data that allows use of the data without being a threat to privacy and that prevents misuse of such data, without significantly altering the accuracy and sensitivity of the identification process (e.g., see specification at page 3, lines 9-14).

For example, the claimed invention compares encrypted data against stored encrypted data while at the same time ensuring that unencrypted data is not available or retrievable under the condition that the data might be slightly different from the template. That is, the claimed invention determines whether P is close to P' by comparing only h(P) with h(P'). Thus, in contrast to conventional methods, the claimed invention compares encrypted data against an encrypted template under the possibility that the data might be slightly different from the template (e.g., "close" to the data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

II. TRAVERSAL OF CLAIM REJECTIONS

For at least the foregoing reasons, Applicants respectfully disagree with the Examiner's positions, and therefore, Applicants traverse each of the Examiner's rejections.

1. FINAL OFFICE ACTION DID NOT RESPOND TO, OR ANSWER THE SUBSTANCE OF, APPLICANTS' TRAVERSAL POSITIONS

It is noted that the Examiner's Response to Arguments in the March 7, 2006 Office Action was identical to the previous Response to Arguments in the September 16, 2005 Office Action, except for stating that:

> *The Applicant failed to provide sufficient evidence to assert the invention's operability, therefore, the 101 rejection stands.*

(see Office Action mailed March 7, 2005, at page 2, paragraph 5).

However, the Examiner did not state *why* or *how* the evidence presented by Applicants, or for that matter, the specifically identified disclosures in the present application which clearly contradict the Examiner's interpretation of the invention, and which clearly rebut the basis of the Examiner's assertion of inoperability, were not sufficient to show operability, or to rebut the Examiner's assertion.

Indeed, with respect to the text of each of the rejections in the present Office Action which were maintained (i.e., the rejection under 35 U.S.C. § 101 and 35 U.S.C. § 103), the above statement at paragraph 5 of the present Office Action was the only difference from the Response to Arguments of the previous Office Action mailed on September 16, 2005. Moreover, the text of the rejections under 35 U.S.C. § 101 and 35 U.S.C. § 103 was identical to the rejections set forth in the previous Office Action.

Thus, Applicants submitted in the Request for Reconsideration under 37 C.F.R. § 1.116 filed on May 8, 2006, and the Appeal Brief filed on September 7, 2006, that the March 7, 2006 Office Action failed to advance the prosecution of the present application.

Applicants argued that, even assuming *arguendo* that the above statement at paragraph 5 of the present Office Action satisfied the requirement for responding to the traversal positions for the rejection under 35 U.S.C. § 101, the Office Action mailed March 7, 2006 clearly failed to take note of or answer the substance of Applicant's traversal positions with respect to the rejection under 35 U.S.C. § 103.

Applicants noted that, where Applicants traverse any rejections, the Examiner should, if he repeats the rejection, take note of the Applicants' argument and answer the substance of it (see M.P.E.P. § 707.07(f)).

The importance of answering Applicants' arguments is illustrated by In re Herrmann, 261 F.2d 598, 120 USPQ 182 (CCPA 1958) where the applicant urged that the subject matter claimed produced new and useful results. The court noted that since applicant's statement of advantages was not questioned by the examiner or the Board of Appeals, it was constrained to accept the statement at face value and therefore found certain claims to be allowable. See also In re Soni, 54 F.3d 746, 751, 34 USPQ2d 1684, 1688 (Fed. Cir. 1995) (Office failed to rebut applicant's argument).

In the Amendment under 37 C.F.R. § 1.111 filed on December 16, 2005, Applicants clearly rebutted each of the Examiner's positions. However, the Examiner did not take note of, or answer the substance of, Applicants' traversal arguments, with the exception of the statement mentioned above.

Applicants respectfully submitted that the Examiner should have responded to all of Applicants' traversal positions and answered the substance of the arguments (e.g., see M.P.E.P. § 707.07(f); see also M.P.E.P. § 2144.08(III)).

That is, the Examiner should have responded to each of Applicants' traversal positions with respect to the rejection under 35 U.S.C. § 101 on pages 16-19 of the Amendment under 37 C.F.R. § 1.111 filed on December 16, 2005.

Moreover, the Examiner should have responded to each of Applicants' traversal positions with respect to the rejection under 35 U.S.C. § 103 on pages 21-26 of the Amendment under 37 C.F.R. § 1.111 filed on December 16, 2005.

For at least the foregoing reasons, Applicants submitted that the March 7, 2006 Office Action failed to advance the prosecution of the present application.

Examiner's Answer

As mentioned above, in the Examiner's Answer mailed November 13, 2006, the Examiner maintained the rejections of Claims 1, 14-16, 31, and 32 under 35 U.S.C. § 101, and Claims 1 and 5-36 under 35 U.S.C. § 103(a) as being unpatentable over Borza in view of Kharon.

The Examiner's Answer dated November 13, 2006 also included a Response to Arguments which addressed the substance of Applicants' traversal positions for the first time, as requested by Applicants in the Amendment under 37 C.F.R. § 1.111 filed on December 16, 2005, the Request for Reconsideration under 37 C.F.R. § 1.116 filed on May 8, 2006, and the Appeal Brief filed on September 7, 2006.

Applicants Traverse Each of the Examiner's Rejections

Applicants now rebut the Examiner's Response to Arguments, as set forth in the Examiner's Answer dated November 13, 2006, and traverse each ground of rejection, for the following reasons.

2. REJECTION OF CLAIMS 1, 14-16, 31, AND 32 UNDER 35 U.S.C. § 101

Claims 1, 14-16, 31, and 32 stand rejected under 35 U.S.C. § 101 as allegedly being inoperative and lacking utility. That is, the Examiner asserted that the claimed invention "*could not work*", as evidenced by the Handbook of Applied Cryptography.

Applicants respectfully disagree with each of the Examiner's positions, for the following reasons.

a) FINAL OFFICE ACTION DID NOT RESPOND TO, OR ANSWER THE SUBSTANCE OF, APPLICANTS' TRAVERSAL POSITIONS

First, as mentioned above, the Examiner's Response to Arguments in the final Office Action dated March 7, 2006, was identical to the previous Response to Arguments in the Office Action dated September 16, 2005, except for stating that "*[t]he Applicant failed to provide sufficient evidence to assert the invention's operability, therefore, the 101 rejection stands*" (see Office Action at page 2, paragraph 5), as mentioned above.

However, Applicants respectfully submitted that such was not sufficient for responding to each of Applicants' traversal positions or answering the substance of those positions (e.g., see M.P.E.P. § 707.07(f) and § 2144.08(III)).

Hence, Applicants respectfully submitted that the Examiner should have responded to all of Applicants' traversal positions and answered the substance of the arguments (e.g., see M.P.E.P. § 707.07(f); see also M.P.E.P. § 2144.08(III)).

b) EXAMINER DID NOT CONSIDER APPLICANTS' ACTUAL ARGUMENT OR THE ACTUAL DISCLOSURE OF THE INVENTION

Second, Applicants respectfully submitted that the Examiner was misunderstanding the invention and Applicants' traversal arguments. Moreover, the Examiner had misapplied the teachings of the Handbook of Applied Cryptography, in view of this apparent misunderstanding of Applicants' traversal position.

Applicants submitted that the disclosure of the present application **explicitly acknowledges** the problem that a simple hash function approach would not work (as disclosed in the above Handbook and as suggested by the Examiner in the March 7, 2006 Office Action at page 4, numbered paragraph 11)(e.g., see specification at page 16, lines 15-17).

Specifically, the specification of the present application (at page 16, lines 15-17) states that:

> Because *P0* is in general (possibly) slightly different form *Pi* for *i>0*, the secret version of *p0* will generally be quite different from the secret version of *Pi*. This is because cryptographic functions are extremely sensitive to the input, thereby to be resilient to attempts to decode the encrypted data. In this case, no identification is possible by direct comparison of the encrypted data (emphasis added).

Accordingly, the present application discloses several approaches to compare encrypted or hashed data **under uncertainty** (e.g., see specification at page 16, line 18 to page 20, line 8).

That is, the specification specifically describes three basis methods **to circumvent the above situation** and the sensitivity of the cryptographic functions (e.g., see specification at page 16, lines 18-19). Indeed, pages 17-20 of the specification specifically describe a first exemplary method, a second exemplary method, and a third exemplary method **for circumventing the very problem** with comparing encrypted or hash data, which the Examiner mentions in the Office Action.

Thus, Applicants argued that the Examiner's continued assertion that the invention is inoperable because of the teachings of the Handbook of Applied Cryptography and section 9.2.2 Basis Properties and Definitions clearly was erroneous, as a matter of both fact and law. That is, the Examiner had failed to consider the specific disclosure of the present application, which clearly describes a novel **solution for circumventing the problem** being relied upon by the Examiner in the Handbook of Applied Cryptography.

Indeed, the disclosure of the present application clearly does not contradict the teachings of the Handbook of Applied Cryptography, upon which the Examiner relies.

Instead, the present invention clearly explains a method of **circumventing** the very problems which the Handbook of Applied Cryptography identifies and for which the Handbook is being relied upon by the Examiner as teaching.

Indeed, Applicants argued that the Examiner had erroneously interpreted what the invention teaches in a way that clearly did not comport with the actual disclosure of the present application.

For example, in paragraph 11 of the March 7, 2006 Office Action, the Examiner stated that the claims "*generally relate to …*". Thus, the Examiner appeared to have improperly attempted to distill the invention down to a gist of the invention.

However, the Examiner's position clearly failed to consider all of the teachings of the invention (i.e., the actual disclosure of the present application), or for that matter, the specific features recited in the claims.

As Applicants have explained in each of the previous Amendments and the Appeal Brief, the claimed invention compares encrypted data against stored encrypted data while at the same time ensuring that unencrypted data is not available or retrievable under the condition that the data might be slightly different from the template. That is, the claimed invention determines whether P is close to P' by comparing only h(P) with h(P') (e.g., see specification at page 16, lines 12-17, and pages 17-20).

(The traversal arguments set forth in the Amendment under 37 C.F.R. § 1.111 filed on June 18, 2004, the Amendment under 37 C.F.R. § 1.116 filed on January 18, 2005, the Amendment under 37 C.F.R. § 1.111 filed on April 15, 2005, the Amendment under 37 C.F.R. § 1.116 filed on July 11, 2005, and the Amendment under 37 C.F.R. § 1.111 filed on December 16, 2005, and the Appeal Brief filed on September 7, 2006, each are incorporated herein by reference in their entirety.)

Thus, the present application explains that, in contrast to conventional methods, the claimed invention compares encrypted data against an encrypted template under the possibility that the data might be slightly different from the template (e.g., "close" to the data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

Indeed, the claimed invention does not merely "generally relate to comparing two separate, imperfect samples of biometric data using a hash function to provide authentication", as alleged by the Examiner.

That is, the claimed invention does NOT use a hash function by ITSELF to authenticate two samples, as erroneously alleged by the Examiner. Instead, a hash function is only part of the novel solution provided by the present invention for circumventing the identified problems with the prior art.

Moreover, not all of the claims deal with imperfect biometric data. Instead, only some of the claims deal with such imperfect data.

For the foregoing reasons, Applicants respectfully submitted that the claimed invention could (and does) work for its intended purpose, as disclosed in the disclosure of the present application (e.g., see specification at page 16, lines 12-17, and page 17, line 1, to page 20, line 8).

Moreover, the present application specifically states that the claimed invention provides a method and system of processing semiotic data that allows use of the data without being a threat to privacy and that prevents misuse of such data, without significantly altering the accuracy and sensitivity of the identification process (e.g., see specification at page 3, lines 9-14).

The specification specifically discloses comparing encrypted data against stored encrypted data while at the same time ensuring that unencrypted data is not available or retrievable under the condition that the data might be slightly different from the template. That is, the claimed invention determines whether P is close to P’ by comparing only h(P) with h(P’). The specification states that, in contrast to conventional methods, the claimed invention compares encrypted data against an encrypted template under the possibility that the data might be slightly different from the template (e.g., "close" to the data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

Thus, contrary to the Examiner's position, Applicants respectfully submitted that claims 1, 14-16, 31, and 32:

> **(1)** are supported by a specific and substantial asserted utility or a well established utility,
>
> **(2)** are not inoperative and do not lack utility, and
>
> **(3)** could (and do) work for their intended purpose, as disclosed in the disclosure of the specification of the present application, for example, at page 16, lines 12-17, and page 17, line 1, to page 20, line 8.

Applicants argued that the Examiner had not explained why the Examiner doubts the truth or veracity of Applicants' disclosure.

To summarize, the Examiner clearly had not responded to all of Applicants' traversal positions or answered the substance of the above traversal arguments (e.g., see M.P.E.P. § 707.07(f); see also M.P.E.P. § 2144.08(III)). Moreover, the Examiner appeared to have erroneously summarized the teachings of the present invention in a way which clearly does not comport with the actual disclosure of the invention. Indeed, the present invention clearly is not contrary to the teachings of the Handbook of Applied Cryptography, but instead, acknowledges the very problem identified in the Handbook by the Examiner and provides a novel solution for circumventing such problems.

Thus, Applicants argued that the Examiner's assertion that "Applicant failed to provide sufficient evidence to assert the invention's operability, therefore, the 101 rejection stands" (see Office Action at page 2, paragraph 5) clearly was inappropriate, and indeed, was <u>not</u> germane to the rejections since the Examiner had <u>not</u> explained or provided any reasons as to why the actual disclosure of the present application would be inoperative and lack utility.

For the foregoing reasons, Applicants respectfully submitted that a person of ordinary skill in the art to which the invention pertains would recognize the utility of the claimed invention and would know and understand the claimed invention. Thus, the Examiner was requested to reconsider and withdraw this rejection.

c) EXAMINER'S ANSWER

In the Examiner's Answer dated November 13, 2006, the Examiner maintains the rejection of Claims 1, 14-16, 31, and 32 under 35 U.S.C. 101 because the disclosed invention allegedly is inoperative and therefore lacks utility.

d) APPLICANTS TRAVERSE THE REJECTION

Applicants traverse this rejection, for at least the following reasons.

i) <u>First</u>, Applicants note that the Response to Arguments in the Examiner's Answer has addressed the substance of Applicants' traversal positions set forth in the Amendment under 37 C.F.R. § 1.111 filed on December 16, 2005, the Request for Reconsideration under 37 C.F.R. § 1.116 filed on May 8, 2006, and the Appeal Brief filed on September 7, 2006, <u>for the first time</u>.

Applicants respectfully submit that the Examiner properly should have responded to all of Applicants' traversal positions and answered the substance of those arguments, in accordance with M.P.E.P. § 707.07(f) and M.P.E.P. § 2144.08(III)), in response to the

Amendment under 37 C.F.R. § 1.111 filed on December 16, 2005, and the Request for Reconsideration under 37 C.F.R. § 1.116 filed on May 8, 2006.

That is, Applicants respectfully submit that the Examiner's positions and Response to Arguments properly should have been set forth earlier in the prosecution, instead of in response to Applicants' Appeal Brief filed on September 7, 2006, such that Applicants would have had a fair and reasonable opportunity to respond to the Examiner's positions prior to having paid the U.S.P.T.O. fees for filing a Notice of Appeal and an Appeal Brief, in the present application.

ii) Second, with respect to the Examiner's Response to Arguments, Applicants traverse this rejection, for at least the following reasons.

In the Response to Arguments of the Examiner's Answer, the Examiner stated that:

> In response to the Appellant's position that the Examiner did not respond to or answer the substance of the Appellant's traversal, the Examiner disagrees. In response to a proper 35 U.S.C. 101 rejection, the burden shifts to the appellant to rebut the prima facie showing. The Appellant may rebut this rejection using any combination of the following: amendments to the claims, arguments or reasoning, or new evidence submitted in an affidavit or declaration under 37 CFR 1.132, or in a printed publication.

(see Examiner's Answer at page 13; emphasis added Applicants).

In the Response to Arguments, the Examiner further stated that:

> In response to the requirement, the Appellant did not amend the claims, submit an affidavit or declaration, or a printed publication to rebut the Examiner's rejection. Instead the Appellant chose to argue by referring back to the specification of the instant application and arguing that the hashes produced are close. The Appellant is reminded that the features upon which appellant relies, such as the methods disclosed in the specification, are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns,* 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The Examiner has considered the specification,

> claims, and prior art before making the rejection and believes the asserted utility would be incredible to a person of ordinary skill in the art. See *In re Rinehart,* 531 F.2d 1048, 1052, 189 USPQ 143, 147 (CCPA 1976).

(see Examiner's Answer at page 13; emphasis added Applicants).

Next, in the Response to Arguments, the Examiner stated that:

> The Appellant failed to properly address the Examiner's *prima facie* showing of the inoperability of the instant invention and the Examiner responded in the only method available at the time, and as such the rejection should be maintained.

(see Examiner's Answer at page 13; emphasis added Applicants).

Applicants respectfully disagree.

Applicants submit that, as the Examiner acknowledged, Applicants may rebut the rejection using any combination of amendments to the claims, arguments or reasoning, or new evidence submitted in an affidavit or declaration under 37 CFR 1.132, or in a printed publication. Next, the Examiner acknowledged that "the Appellant chose to argue by referring back to the specification of the instant application and arguing that the hashes produced are close" (see Examiner's Answer at page 13; emphasis added Applicants).

Thus, it is unclear to Applicants how the Examiner then takes the position that "Appellant failed to properly address the Examiner's *prima facie* showing of the inoperability of the instant invention". Indeed, the Examiner's statement seems to be contrary to the previous statements, which indicate that Applicants did address the Examiner's alleged prima facie case.

Accordingly, Applicants respectfully reiterate that the Examiner properly should have taken note of and answered the substance of Applicants' traversal positions.

iii) Turning again to the Response to Arguments in the Examiner's Answer, the Examiner states that:

> In response to the Appellant's arguments that the Examiner is not considering the Appellant's actual argument or the actual disclosure of the invention, the Examiner disagrees. The Appellant agrees with the Examiner's position that a simple hash function would not work on page 26 of the Appeal Brief filed 07 September 2006. The Appellant refers to methods for circumventing the problems of comparing encrypted or hashed data samples **<u>but is reminded that the features upon which appellant relies are not recited in the rejected claims</u>**. Although <u>the claims are interpreted in light of the specification, limitations from the specification are not read into the claims</u>. See *In re Van Geuns,* 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

(see Examiner's Answer at page 14, last paragraph; emphasis added Applicants).

<u>Applicants respectfully disagree.</u>

Contrary to the Examiner's position, Applicants respectfully submit that the features upon which Applicants rely <u>clearly are recited in the rejected claims</u>.

<u>Independent claim 1</u>

For example, turning to the specific language of independent claim 1, the claimed invention recites a method of processing semiotic data, including:

> *receiving semiotic data including at least one data set P;*
> *selecting a function h, and for at least one of each said data set P to be collected, computing h(P);*
> *destroying said data set P;*
> *storing h(P) in a database, and*
> *obtaining a sample of P' such that a comparison can be made;*
> *at least one of obtaining and computing h(P'); and*
> ***<u>to determine whether P' is close to a predetermined subject, comparing h(P') to available h(P)s to determine whether P' substantially matches, but does not exactly match, one of said data set P,</u>***
> *wherein said data set P cannot be extracted from h(P),*
> *wherein said semiotic data comprises biometric data,*
> *wherein said function h comprises a secure hash function,*
> *<u>wherein the data set P is not determined perfectly by its reading,</u>*

> *wherein each reading gives a number Pi, wherein i is no less than 0, wherein P0 is for an initial reading, and a secret version of said initial reading is stored after further processing thereof,*
>
> *wherein reading P0 is different from Pi for i > 0, and the secret version of P0 is different from the secret version of Pi, such that no identification is possible by a direct comparison of the encrypted data,*
>
> *said method further comprising:*
>
> *extracting sub-collections Sj from the collection of data in data set P;*
>
> *encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability,*
>
> ***comparing encrypted versions of the sub-collections Sj with those data stored in said database,***
>
> ***wherein if one or more of the sub-collection Sj matches with said data, then verification is deemed to have occurred,***
>
> *each time a Pi, with i > 0, is read, computing all possible predetermined size variations of Pi which correspond to an acceptable predetermined imprecision of the reading; and*
>
> *encrypting all such modified data, and comparing said encrypted modified data to data stored in said database,*
>
> *wherein for a plurality of users of the same biometric information, said biometric information is encrypted differently for each user, and*
>
> *wherein at least one of said data set P and P' comprises a personal data set* (emphasis added Applicants).

Thus, independent claim 1 clearly defines a method in which, "*to determine whether P' is close to a predetermined subject, comparing h(P') to available h(P)s to determine whether P' substantially matches, but does not exactly match, one of said data set P*" (emphasis added Applicants). Independent claims 15 and 32 recite somewhat similar features.

Moreover, independent claim 1 further recites "*extracting sub-collections Sj from the collection of data in data set P; encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined* *probability, comparing encrypted versions of the sub-collections Sj with those data stored in said database, wherein if one or more of the sub-collection Sj matches with said data, then verification is deemed to have occurred*" (emphasis added Applicants).

Contrary to the Examiner's position, Applicants submit that the features which are described at pages 17-20 of the present application are, in fact, recited by independent claim 1. Thus, Applicants' traversal positions were directed to the claim language and these features properly should have been considered by the Examiner.

Applicants also note that Claim 14 depends from claim 1, and therefore, is traversed for somewhat similar reasons.

Hence, the Examiner's position that the "Appellant refers to methods for circumventing the problems of comparing encrypted or hashed data samples but is reminded that the features upon which appellant relies are not recited in the rejected claims" is not understood.

For the foregoing reasons, Applicants respectfully reiterate that the claimed invention could (and does) work for its intended purpose, as disclosed in the disclosure of the present application (e.g., see specification at page 16, lines 12-17, and page 17, line 1, to page 20, line 8).

Moreover, the present application specifically states that the claimed invention provides a method and system of processing semiotic data that allows use of the data without being a threat to privacy and that prevents misuse of such data, without significantly altering the accuracy and sensitivity of the identification process (e.g., see specification at page 3, lines 9-14).

The specification specifically discloses comparing encrypted data against stored encrypted data while at the same time ensuring that unencrypted data is not available or retrievable under the condition that the data might be slightly different from the template. That is, the claimed invention determines whether P is close to P' by comparing only h(P) with h(P'). The specification states that, in contrast to conventional methods, the claimed invention compares encrypted data against an encrypted template under the possibility that the data might be slightly different from the template (e.g., "close" to the data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

Thus, contrary to the Examiner's position, Applicants respectfully reiterate that claims 1, 14-16, 31, and 32:

(1) are supported by a specific and substantial asserted utility or a well established utility,
(2) are not inoperative and do not lack utility, and
(3) could (and do) work for their intended purpose,

as disclosed in the disclosure of the specification of the present application, for example, at page 3, lines 9-14, page 16, lines 12-17, and page 17, line 1, to page 20, line 8.

Applicants reiterate that, to date, the Examiner has not explained why the Examiner doubts the truth or veracity of Applicants' disclosure, or provided any reasons as to why the actual disclosure of the present application would be inoperative and lack utility.

For the foregoing reasons, the Examiner was requested to reconsider and withdraw this rejection.

iv) Turning again to the Response to Arguments in the Examiner's Answer, the Examiner states that:

> The Examiner would like to point out that the **Appellant fails to define/redefine the term hash function to coincide with a particular method disclosed in the specification.** Where appellant acts as his or her own lexicographer to specifically define a term of a claim contrary to its ordinary meaning, the written description must clearly redefine the claim term and set forth the uncommon definition so as to put one reasonably skilled in the art on notice that the appellant intended to so redefine that claim term. *Process Control Corp. v. HydReclaim Corp.,* 190 F.3d 1350, 1357, 52 USPQ2d 1029, 1033 (Fed. Cir. 1999). The Appellant has not elaborated in the claim language that the hash function is one of the disclosed methods on pages 17-20 of the specification. The Appellant fails to meet the requirements of redefining a term as set forth in the MPEP § 2106. In order to define/redefine a term, the Appellant must do so "with reasonable clarity, deliberateness, and precision" and must " set out his uncommon definition in some manner within the patent disclosure' so as to give one of ordinary skill in the art notice of the change" in meaning.

(see Examiner's Answer at page 14, last paragraph; emphasis added Applicants).

Contrary to the Examiner's position, Applicants submit that nowhere in the present appliation, or in the previous Responses, have Applicants attempted to define or redefine the term "*hash function*", or be their own lexicographer of the term "*hash function*", or for that matter, assert that the claimed term "*hash function*", by itself, is defined as "one of the disclosed methods on pages 17-20 of the specification" (see Examiner's Answer at page 14, last paragraph).

Instead, Applicants argued that the Examiner was misunderstanding the invention and Applicants' traversal arguments. Moreover, Applicants argued that the Examiner had misapplied the teachings of the Handbook of Applied Cryptography, in view of this apparent misunderstanding of Applicants' traversal position.

Moreover, as mentioned above, Applicants argued, *inter alia*, that the present application discloses several approaches to compare encrypted or hashed data **under uncertainty** (e.g., see specification at page 16, line 18 to page 20, line 8). That is, the specification specifically describes three basis methods **to circumvent the above situation** and the sensitivity of the cryptographic functions (e.g., see specification at page 16, lines 18-19). Indeed, pages 17-20 of the specification specifically describe a first exemplary method, a second exemplary method, and a third exemplary method **for circumventing the very problem** with comparing encrypted or hash data, which the Examiner mentions in the Office Action.

Thus, Applicants argued that the Examiner's continued assertion that the invention is inoperable because of the teachings of the Handbook of Applied Cryptography and section 9.2.2 Basis Properties and Definitions clearly was erroneous, as a matter of both fact and law. That is, the Examiner had failed to consider the specific disclosure of the present application, which clearly describes a novel **solution for circumventing the problem** being relied upon by the Examiner in the Handbook of Applied Cryptography. Indeed, the disclosure of the present application clearly does not contradict the teachings of the Handbook of Applied Cryptography, upon which the Examiner relies.

Instead, the present invention clearly explains a method of **circumventing** the very problems which the Handbook of Applied Cryptography identifies and for which the Handbook is being relied upon by the Examiner as teaching.

As Applicants have explained in each of the previous Amendments and the Appeal Brief, the claimed invention compares encrypted data against stored encrypted data under the condition that the data might be slightly different from the template. That is, the claimed invention determines whether P is close to P' by comparing only h(P) with h(P') (e.g., see specification at page 16, lines 12-17, and pages 17-20).

Thus, the present application explains that, in contrast to conventional methods, the claimed invention compares encrypted data against *an encrypted template* under the possibility that the data might be slightly different from the template (e.g., "close" to the data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

That is, the claimed invention does NOT use a hash function by ITSELF to authenticate two samples, as erroneously alleged by the Examiner. Instead, a hash function is only part of the novel solution provided by the present invention for circumventing the identified problems with the prior art.

Thus, it is unclear how the Examiner's Response to Arguments, or the cited case law with respect to defining claim terms, is germane to this rejection.

For the foregoing reasons, the Examiner is requested to reconsider and withdraw this rejection.

v) Next, in the Response to Arguments, the Examiner stated that:

> The Examiner has considered the claim language as a whole and in light of the specification, and has refrained from reading limitations from the specification into the claim language, especially giving the "hash function" its broadest reasonable interpretation. The Examiner does not disagree with the Appellant that the disclosure of the invention is operable, but the claim language as broadly interpreted by the Examiner provides for an inoperable invention and the rejection should be maintained.

(see Examiner's Answer at page 14; emphasis added Applicants).

Applicants respectfully submit that the Examiner's position is not understood.

First, as set forth in M.P.E.P. § 2111, during patent examination, the pending claims must be "given their broadest reasonable interpretation consistent with the specification."

(emphasis added Applicants). The Federal Circuit's *en banc* decision in Phillips v. AWH Corp., 415 F.3d 1303, 75 USPQ2d 1321 (Fed. Cir. 2005) expressly recognized that the USPTO employs the "broadest reasonable interpretation" standard:

> The Patent and Trademark Office ("PTO") determines the scope of claims in patent applications not solely on the basis of the claim language, but upon giving claims their broadest reasonable construction "in light of the specification as it would be interpreted by one of ordinary skill in the art." In re Am. Acad. of Sci. Tech. Ctr., 367 F.3d 1359, 1364[, 70 USPQ2d 1827] (Fed. Cir. 2004). Indeed, the rules of the PTO require that application claims must "conform to the invention as set forth in the remainder of the specification and the terms and phrases used in the claims must find clear support or antecedent basis in the description so that the meaning of the terms in the claims may be ascertainable by reference to the description." 37 CFR 1.75(d)(1). 415 F.3d at 1316, 75 USPQ2d at 1329.

Applicants also note that "reading a claim in light of the specification, to thereby interpret limitations explicitly recited in the claim, is a quite different thing from 'reading limitations of the specification into a claim,' to thereby narrow the scope of the claim by implicitly adding disclosed limitations which have no express basis in the claim." See In re Prater, 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-51 (CCPA 1969)

In this case, Applicants submit that the Examiner's broad interpretation is not a reasonable interpretation, in view of the specification.

That is, the Examiner specifically concedes that "the disclosure of the invention is operable". Thus, it is unclear how the explicitly recited features of independent claims 1, 15, and 32, which clearly recite a method in which, "*to determine whether P' is close to a predetermined subject, comparing h(P') to available h(P)s to determine whether P' substantially matches, but does not exactly match, one of said data set P*", and which correspond to the features of the invention described, for example, at pages 17-20, could reasonably be interpreted to not be operable when interpreted in light of the specification.

Moreover, if, as the Examiner concedes, “the disclosure of the invention is operable”, then it is unclear how the explicitly recited features of independent claim 1, which further recites a method including *extracting sub-collections Sj from the collection of data in data set P; encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability, comparing encrypted versions of the sub-collections Sj with those data stored in said database, wherein if one or more of the sub-collection Sj matches with said data, then verification is deemed to have occurred*” (emphasis added Applicants), would not be operable when reasonably interpreted in light of the specification.

Again, the Examiner concedes that “the disclosure of the invention is operable”.

However, the Examiner has not identified or establish what information allegedly is missing from the claims (e.g., independent claim 1), which would result in such a broad interpretation of the claims that renders independent claim 1 inoperable in view of the operable disclosure.

Applicants submit that interpreting the explicitly recited features of the claims in a manner that would render the claims inoperable, and thus, in manner that is broader than the actual disclosure of the application, would not be a reasonably broad interpretation, particularly, since the actual disclosure is conceded to be operable (e.g., see specification at pages 17-20).

That is, Applicants submit that it would not be reasonable to interpret the above-identified recitations of independent claim 1 so broadly that they are rendered inoperable, despite the features of the disclosure which are conceded to be operable.

On the contrary, Applicants submit that the ordinarily skilled artisan reasonably would consider the explicitly recited features of the claims to be operable in view of the operable disclosure (e.g., see specification at pages 17-20).

For the foregoing reasons, the Examiner is requested to reconsider and withdraw this rejection.

3. THE PRIOR ART REJECTION UNDER 35 U.S.C. § 103

Claims 1 and 5-36 previously stood rejected under 35 U.S.C. § 103(a) as being unpatentable over Borza in view of Kharon. However, in the Examiner Answer, the rejection was revised such that Claims 1, 5-8, 10-14, 16, 18-26, 28-32, and 34-36 now stand rejected under 35 U.S.C. 103(a) as being unpatentable over Borza in view of Kharon.

Applicants respectfully traverse this rejection, for at least the following reasons.

As mentioned above, the traversal arguments set forth in the Amendment under 37 C.F.R. § 1.111 filed on June 18, 2004, the Amendment under 37 C.F.R. § 1.116 filed on January 18, 2005, the Amendment under 37 C.F.R. § 1.111 filed on April 15, 2005, the Amendment under 37 C.F.R. § 1.116 filed on July 11, 2005, the Amendment under 37 C.F.R. § 1.111 filed on December 16, 2005, and the Appeal Brief filed on September 7, 2006, are incorporated herein by reference in their entirety.

a) THE CLAIMED INVENTION

The claimed invention provides a method and system of processing semiotic data that allows use of the data without being a threat to privacy and that prevents misuse of such data, without significantly altering the accuracy and sensitivity of the identification process (e.g., see specification at page 3, lines 9-14).

For example, the claimed invention compares encrypted data against stored encrypted data while at the same time ensuring that unencrypted data is not available or retrievable under the condition that the data might be slightly different from the template. That is, the claimed invention determines whether P is close to P' by comparing only h(P) with h(P'). Thus, in contrast to conventional methods, the claimed invention compares encrypted data against an encrypted template under the possibility that the data might be slightly different from the template (e.g., "close" to the data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

b) EXAMINER'S RESPONSE TO ARGUMENTS

In the "Response to Arguments" section of the final Office Action, the Examiner continued to allege that the features upon which Applicants rely are not recited in the claims (see Office Action at page 3, paragraph 6). However, Applicants submitted that the traversal arguments which are set forth at least in the Amendment under 37 C.F.R. § 1.111 filed on April 15, 2005 and the Amendment under 37 C.F.R. § 1.116 filed on July 11, 2005, clearly point out the claimed subject matter which is clearly and particularly defined, for example, by independent claim 1.

Also, in the "Response to Arguments" section of the final Office Action, the Examiner relied on M.P.E.P. § 2122 as stating that, when a reference relied upon expressly anticipates or makes obvious all of the elements of the claimed invention, the reference is presumed to be operable.

c) EXAMINER'S POSITION IN THE FINAL OFFICE ACTION WAS FLAWED AS A MATTER OF FACT AND LAW

Applicants respectfully submitted that the Examiner's position in the final Office Action was flawed as a matter of fact and law.

First, as Applicants have pointed out, Borza does not expressly anticipate or make obvious all of the elements of the claimed invention. Thus, irrespective of the operability of Borza, Applicants submit that the alleged combination of Borza and Kharon does not disclose or suggest all of the features of the claimed invention.

Instead, Borza only generally mentions that a comparison of encrypted data is done, but does not disclose the specific features recited in the claimed invention. In fact, Borza clearly does not discuss *how* it compares encrypted data.

In fact, the cited portion of Borza at column 16, lines 31-38 does not determine whether h(P) is close to h(P'), as alleged by the Examiner. Indeed, it is unclear how Borza at column 16, lines 31-38 even relates to the disclosure of comparing encrypted data against an encrypted template at column 8, lines 28-38.

That is, nowhere at column 16, lines 31-38, or in Figure 13 which is being described therein, does Borza mention comparing encrypted data against an encrypted template. Thus, the Examiner has mischaracterized the teachings of Borza.

Second, even assuming *arguendo* that Borza is operative, the disclosure provided by Borza fails to teach or suggest all of the features of the claimed invention for which it is being relied upon. Therefore, the alleged combination of Borza and Kharon clearly does not disclose or suggest all of the features of the claimed invention.

In other words, irrespective of the operability of Borza, the disclosure of Borza clearly does not disclose or suggest *how* to compare two encrypted data sets to determine similarity between the two original data sets according to the features recited in the claimed invention.

Applicants reiterated that the ordinarily skilled artisan would understand that encryption causes diffusion of data, which means that the encryption of two similar, but not identical data sets create two encrypted data sets that are very different. Thus, merely comparing two encrypted data sets still would not (and does not) disclose or suggest the similarity between the two unencrypted data sets.

In fact, as the Examiner pointed out, and as Applicants specifically acknowledge in the specification, no identification is possible by direct comparison of the encrypted data.

Thus, in contrast to Borza, the claimed invention discloses several approaches to compare encrypted or hashed data **under such uncertainty** (e.g., see specification at page 16, line 18 to page 20, line 8).

Specifically, as mentioned above, the disclosure of the present invention specifically acknowledges the problem that a simple hash function approach would not work (as suggested by the Examiner in the Office Action at page 4, numbered paragraph 11)(e.g., see specification at page 16, lines 15-17).

For example, the specification of the present application (at page 16, lines 15-17) specifically states that:

> Because *P0* is in general (possibly) slightly different form *Pi* for *i>0*, the secret version of *p0* will generally be quite different from the secret version of *Pi*. This is because cryptographic functions are extremely sensitive to the input, thereby to be resilient to attempts to decode the encrypted data. In this case, no identification is possible by direct comparison of the encrypted data (emphasis added).

Accordingly, the present application discloses several approaches to compare encrypted or hashed data **under such uncertainty** (e.g., see specification at page 16, line 18 to page 20, line 8).

That is, the specification specifically describes three basis methods **to circumvent this situation** and the sensitivity of the cryptographic functions (e.g., see specification at page 16, lines 18-19). Indeed, pages 17-20 of the specification specifically describe first, second, and third methods for circumventing the very problem with comparing encrypted or hash data which the Examiner mentions.

The claimed invention compares encrypted data against stored encrypted data while at the same time ensuring that unencrypted data is not available or retrievable under the condition that the data might be slightly different from the template. That is, the claimed invention determines whether P is close to P' by comparing only h(P) with h(P') (e.g., see specification at page 16, lines 12-17, and pages 17-20).

The present application explains that, in contrast to conventional methods, the claimed invention compares encrypted data against an encrypted template *under the* *possibility that the data might be slightly different from the template* (e.g., "close" to the data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

Thus, the claimed invention solves the problem that a simple hash function approach would not work (as suggested by the Examiner in the Office Action at page 4, numbered paragraph 11)(e.g., see specification at page 16, lines 15-17) by circumventing the problem, as disclosed and claimed.

For the foregoing reasons, Borza clearly does not disclose or suggest at least "*to determine whether P' is close to a predetermined subject, comparing h(P') to available h(P)s to determine whether P' substantially matches, but does not exactly match, one of said data set P*", as recited in claim 1.

Independent claims 5, 9, 15, 17, 19, 24, 27, 29, 31, 33, and 35 recite somewhat similar features. Therefore, Applicants submitted that Independent claims 5, 9, 15, 17, 19, 24, 27, 29, 31, 33, and 35 also are patentable over the prior art of record for the same reasons as independent claim 1.

On the other hand, Applicants respectfully reiterated that Kharon does not make up for the deficiencies of Borza.

The Examiner relied on Kharon for teaching the claimed "*extracting sub-collections Sj from the collection of data in data set P; encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability, comparing encrypted versions of the sub-collections Sj with those data stored in said database, wherein if one or more of the sub-collection Sj matches with said data, then verification is deemed to have occurred*", as recited in independent claim 1.

However, contrary to the Examiner's position, Kharon (at column 13, lines 43-67) does not describe extracting multiple subsets Sj (i.e., "*sub-collections*") from the data. Furthermore, Kharon does not describe encrypting a number of such subsets (i.e., a "*number of such sub-collections*") such that at least one is reproduced exactly with a predetermined probability.

Applicants respectfully submitted that the Examiner seemed to have confused using a smaller section of the data for verification (which would be less desirable since less data is used), whereas the claimed invention uses multiple subsets of the data for verification.

Thus, using just a smaller subset of the data for verification would be less desirable since it is easy to forge the data and does not solve the problem of being able to compare two encrypted data.

On the other hand, using multiple subsets of the data, according to the claimed invention, allows encrypted data to be compared and to generate a measure of similarity.

Thus, for the foregoing reasons, Applicants respectfully submitted that Borza and Kharon, either individually or in combination, discloses or suggests all of the features of the claimed invention. Therefore, the Examiner was requested to reconsider and withdraw this rejection. In view of all of the foregoing, Applicants submitted that all of the pending claims (i.e., claims 1 and 5-36) are patentable over the prior art of record.

d) EXAMINER'S ANSWER

In the Examiner's Answer, the Examiner revised the rejection of Claims 1 and 5-36 under 35 U.S.C. § 103(a) as being unpatentable over Borza in view of Kharon, to limit the rejected claims to Claims 1, 5-8, 10-14, 16, 18-26, 28-32, and 34-36.

Thus, Claims 1, 5-8, 10-14, 16, 18-26, 28-32, and 34-36 now stand rejected under 35 U.S.C. 103(a) as being unpatentable over Borza in view of Kharon.

e) APPLICANTS TRAVERSE THE REJECTION

Applicants traverse this rejection, for at least the following reasons.

First, Applicants note that the Response to Arguments in the Examiner's Answer has addressed the substance of Applicants' traversal positions set forth in the Amendment under 37 C.F.R. § 1.111 filed on December 16, 2005, the Request for Reconsideration under 37 C.F.R. § 1.116 filed on May 8, 2006, and the Appeal Brief filed on September 7, 2006, for the first time.

Applicants respectfully submit that the Examiner properly should have responded to all of Applicants' traversal positions and answered the substance of those arguments, in accordance with M.P.E.P. § 707.07(f) and M.P.E.P. § 2144.08(III)), in response to the Amendment under 37 C.F.R. § 1.111 filed on December 16, 2005, and the Request for Reconsideration under 37 C.F.R. § 1.116 filed on May 8, 2006.

That is, Applicants respectfully submit that the Examiner's positions and Response to Arguments properly should have been set forth earlier in the prosecution, instead of in response to Applicants' Appeal Brief filed on September 7, 2006, such that Applicants would have had a fair and reasonable opportunity to respond to the Examiner's positions prior to having paid the U.S.P.T.O. fees for filing a Notice of Appeal and an Appeal Brief, in the present application.

With respect to the Examiner's Response to Arguments, Applicants traverse this rejection, for at least the following reasons.

In the Examiner's Answer dated November 13, 2006, the Examiner states that:

> In response to appellant's argument that the claimed invention provides a method and system for processing semiotic data that allows use of the data without being a threat to privacy and that prevents misuse of such data, without significantly altering the accuracy and sensitivity of the identification process, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim.

(see Examiner's Answer at page 15).

Applicants respectfully submit, however, that independent claim 1 defines a "method", and therefore, it is unclear how the Examiner's statement is germane to independent claim 1.

In the Examiner's Answer dated November 13, 2006, the Examiner states that:

> In response to appellant's argument that the references fail to show certain features of appellant's invention, it is noted that the features, such as how the comparison between the two data sets are compared, upon which appellant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns,* 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The Appellant does not claim the structure that does the comparing between the two encrypted samples, but instead claims the method steps which the Examiner has shown to be taught by *Borza.*

(see Examiner's Answer at page 15).

Applicants respectfully submit, however, that independent claims 24 and 29 recite "system" claims. Therefore, it is unclear how the Examiner's statement is germane to independent claims 24 and 29.

In the Examiner's Answer dated November 13, 2006, the Examiner further states that:

> In response to the Appellant's arguments that *Borza* does not determine whether h(P) is close to h(P'), the Examiner disagrees. *Borza* discloses at column 16, lines 19-

> 38 discloses techniques for determining the identification of someone by acquiring a biometric sample and comparing it to the stored templates. If the sample acquired for authentication is within predetermined range of the template, identification is provided for, if it is outside that predetermined range, then the user is not authenticated. *Borza* teaches comparing encrypted samples to encrypted templates in column 8, lines 28-38. The Appellant is reminded of MPEP 2123, which states that patents are relevant as prior art for all they contain.

(see Examiner's Answer at page 15).

The Examiner further states that "*Borza* discloses determining whether h(P) is close to h(P'), without having to be identical matches, when comparing encrypted samples to encrypted templates, and the rejection should be maintained." (see Examiner's Answer at page 15).

Applicants respectfully disagree.

First, Borza discloses that "[w]hen a substantial match occurs between a template and the characterized biometric information" (see Borza at column 8, lines 9-12). The characterized biometric information is <u>not</u>, however, encrypted information.

On the other hand, column 8, lines 28-30 describe comparing the encrypted characterized biometric information to against an encrypted template. However, Borza fails to describe how the <u>encrypted</u> information could be compared to determine a substantial match, and indeed, does not state that a substantial match is determined, when Borza describes the encrypted information.

Thus, contrary to the Examiner's position, Borza does <u>not</u> disclose the features for which it is being relied upon.

The Examiner further states that:

> In response to the Appellant's argument that *Kharon* does not disclose extracting multiple subsets of data, the Examiner states that, "In column 14, lines 40-53 *Kharon* discloses the k`" minutia and groupings of minutia. *Kharon* also states at column 13, lines 63-67 that the data set is defined so that N represents the total number of minutia for the fingerprint. *Kharon* discloses extracting multiple subsets from the data in disclosing multiple instances of the minutia, and the rejection should be upheld."

(see Examiner's Answer at page 15).

In response to the Appellant's argument that *Kharon* does not teaches comparing encrypted versions of the sub-collection with those stored in the database, the Examiner disagrees.

The Examiner states that "As shown above, *Borza* provides a showing of comparing two encrypted data sets for authentication purposes. *Kharon* teaches at column 14, lines 1-9 of comparing the minutia data sets to that of a database for authenticating the fingerprint. Therefore, the combination of references discloses comparing encrypted subsets of data against a database for verification and the rejection should be maintained." (see Examiner's Answer at pages 16-17).

Applicants respectfully disagree.

First, the Examiner seems to agree with Applicants that Kharon does not teach comparing encrypted versions of the sub-collection with those stored in the database. Instead, Kharon teaches only comparing unencrypted data. That is, the Examiner now takes the position that the combination of Borza and Kharon teach this feature.

Second, assuming *arguendo* that, as the Examiner asserts, Borza provides a showing of comparing two encrypted data sets for authentication purposes, and that Kharon teaches at comparing the minutia data sets to that of a database for authenticating a fingerprint, Applicants submit that the ordinarily skilled artisan would not have been motivated to combine these features to arrive at the claimed invention, for at least the following reasons.

First, Applicants respectfully submit that the Examiner has not established a *prima facie* motivation for combining these references.

That is, the Examiner alleges that "It would have been obvious to one of ordinary skill in the art at the time the invention was made to sample a smaller section of the data set. One would be motivated to do because there is a better probability that a smaller area is less likely to change, therefore making it more difficult for someone to steal someone's identification" (see Examiner's Answer at page 7).

However, the Examiner does not provide, or cite, any support for the alleged motivation. Indeed, it is unclear whether one or more of the references are deemed to provide the motivation, or if the Examiner is relying on the general knowledge within the art for such motivation.

Thus, as a procedural matter, and as a matter of law, the Examiner has not established a *prima facie* motivation for combining these references.

Applicants note that, "In determining the propriety of the Patent Office case for obviousness in the first instance, it is necessary to ascertain whether or not the reference teachings would appear to be sufficient for one of ordinary skill in the relevant art having the reference before him to make the proposed substitution, combination, or other modification." In re Linter, 458 F.2d 1013, 1016, 173 USPQ 560, 562 (CCPA 1972)" (citing M.P.E.P. § 2143.01).

Moreover, Applicants note that “Obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so >. In re Kahn, 441 F.3d 977, 986, 78 USPQ2d 1329, 1335 (Fed. Cir. 2006) (discussing rationale underlying the motivation-suggestion-teaching requirement as a guard against using hindsight in an obviousness analysis). The teaching, suggestion, or motivation must be< found either explicitly or implicitly in the references themselves or in the knowledge generally available to one of ordinary skill in the art. "The test for an implicit showing is what the combined teachings, knowledge of one of ordinary skill in the art, and the nature of the problem to be solved as a whole would have suggested to those of ordinary skill in the art." In re Kotzab, 217 F.3d 1365, 1370, 55 USPQ2d 1313, 1317 (Fed. Cir. 2000). See also In re Lee, 277 F.3d 1338, 1342-44, 61 USPQ2d 1430, 1433-34 (Fed. Cir. 2002) (discussing the importance of relying on objective evidence and making specific factual findings with respect to the motivation to combine references); In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992)”(citing M.P.E.P. § 2413.01).

Moreover, notwithstanding the above, Applicants respectfully submit that it would not have been obvious to combine these references in the manner alleged, since neither Borza nor Kharon provide any teaching of how such a combination would be made.

It is noted that, although a prior art device "may be capable of being modified to run the way the apparatus is claimed, there must be a suggestion or motivation in the reference to do so." 916 F.2d at 682, 16 USPQ2d at 1432.). See also In re Fritch, 972 F.2d 1260, 23

USPQ2d 1780 (Fed. Cir. 1992) (flexible landscape edging device which is conformable to a ground surface of varying slope not suggested by combination of prior art references).

That is, it is not enough merely to combine the teachings of the references based on the teachings of Applicant's invention (i.e., impermissible hindsight based analysis).

Instead, the Examiner must show that the ordinarily skilled artisan, having read the teachings of Borza and Kharon, would have been motivated, by the references themselves, or the teachings of art in general, to make the claimed combination.

Thus, as a matter of law, the Examiner has not established a *prima facie* motivation for combining these references.

The Examiner also states that "In response to appellant's argument that the claimed invention using a smaller subset of data for verification would be less desirable since it is easy to forge the data and does not solve the problem of being able to compare two encrypted data sets, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim." (see Examiner's Answer at page 17, second full paragraph).

Applicants note, however, that the Examiner's statement mischaracterizes Appellants arguments.

That is, Appellants argued that the Examiner seemed to have confused using a smaller section of the data for verification (which would be less desirable since less data is used), whereas the claimed invention uses multiple subsets of the data for verification. Thus, using just a smaller subset of the data for verification would be less desirable since it is easy to forge the data and does not solve the problem of being able to compare two encrypted data.

On the other hand, using multiple subsets of the data, according to the claimed invention, allows encrypted data to be compared and to generate a measure of similarity.

Applicants also submit that the claimed invention using multiple subsets of the data for verification is not merely a statement of intended use, since the claims explicitly recite using multiple subsets of the data.

For example, independent claim 1 recites "*extracting sub-collections Sj from the collection of data in data set P*" (emphasis added). The term "*sub-collections*" clearly is plural, and thus, means more than one sub-collection is used.

With respect to the Examiner's assertion that "Appellant's arguments fail to comply with 37 CFR 1. 1(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references" (see Examiner's Answer at page 17), Applicants respectfully disagree.

Contrary to the Examiner's position, Applicants submit that Applicants' clearly have pointed out the explicitly recited features of the claims which are believed to be patentable over the cited references, for at least the reasons set forth above.

In the Examiner's Answer, the Examiner further states that:

> In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller,* 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

(see Examiner's Answer at page 17).

Applicants respectfully disagree. It is noted that Applicants traversal of the Examiner's positions with respect to the specific features upon which the Examiner relies on each reference as teaching clearly does not amount to arguing the references individually, as in the cited case law. Indeed, the case law cited by the Examiner is not believed to be pertinent or applicable to the facts in the present application, or for that matter, the context of Applicants traversal arguments in this application.

In the Examiner's Answer, the Examiner further states that:

> In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies, such as extracting subsets of data and comparing encrypted subsets of data, are not recited in all of the rejected independent claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns,* 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

(see Examiner's Answer at page 17).

Applicants note that, to expedite prosecution, the claims have been amended above to include somewhat similar features, where appropriate.

For the foregoing reasons, Applicants submit that claims 1, 5-8, 10-14, 16, 18-26, 28-32, and 34-36 are patentable over Borza and Kharon, either individually or in combination.

Therefore, the Examiner is requested to reconsider and withdraw this rejection.

4. NEW GROUND OF REJECTION OF CLAIMS 31-36 UNDER 35 U.S.C. § 101

Claims 31-36 were newly rejected under 35 U.S.C. 101 as allegedly being directed to non-statutory subject matter.

To expedite prosecution, claims 31-36 are amended to define more clearly the features of the invention, thereby overcoming the rejection under 35 U.S.C. § 101.

Therefore, the Examiner is requested to reconsider and withdraw this rejection.

5. NEW GROUND OF REJECTION OF CLAIMS 1 AND 5-36 UNDER 35 U.S.C. § 102(e)

Claims 9, 15, 17, 27, and 33 were newly rejected under 35 U.S.C. 102(e) as being anticipated by Borza. Applicants respectfully traverse this rejection, for at least the following reasons.

While Applicants believe that all of the claims are patentable over the prior art of record, to expedite prosecution, claims 9, 15, 17, and 33 are amended to define more clearly the features of the invention.

Applicants submit that Borza clearly does not disclose or suggest at least "*extracting sub-collections Sj from the collection of data in data set P*" and "*encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability*", as claimed.

Moreover, Borza clearly does not disclose or suggest at least "*comparing encrypted versions of the sub-collections Sj with those data stored in said database, wherein if one or* *more of the sub-collection Sj matches with said data, then verification is deemed to have occurred*", as claimed.

Therefore, the rejection of these claims should be withdrawn.

With respect to independent claim 27, Applicants note that claim 27 recites the features of the invention using <u>means-plus-function language</u>, which properly should be interpreted as including the specific arrangement of elements disclosed in the specification and drawings (and then "reasonable" equivalents under 35 U.S.C. § 112, sixth paragraph).

Particularly, claim 27 recites, inter alia, "*means <u>for comparing</u> an encrypted data set of a data set P' to said at least one encrypted data set of data set P <u>to determine whether there is a match and to determine whether the data set P' is a predetermined subject</u>*" (emphasis added).

Applicants submit that Borza clearly does <u>not</u> disclose or suggest any structure, equivalents thereof, or identity of function necessary for the claimed "*means <u>for comparing</u>*", as disclosed in the present application at, for example, pages 17-20.

Thus, the Examiner is requested to reconsider and withdraw this rejection.

6. EXAMINER'S ANSWER, INCLUDING NEW GROUNDS OF REJECTION, WAS <u>NOT</u> SIGNED BY TECHNOLOGY CENTER DIRECTOR

As mentioned above, the Examiner's Answer dated November 13, 2006 raised two new grounds of rejection. That is, Claims 31- 36 were newly rejected under 35 U.S.C. 101 as allegedly being directed to non-statutory subject matter, and Claims 9, 15, 17, 27, and 33 were newly rejected under 35 U.S.C. 102(e) as being anticipated by Borza.

The Examiner's Answer, at page 19, noted that a Technology Center Director or designee must personally approve the new ground(s) of rejection set forth in section (9) above by signing the Examiner's Answer.

The Examiner's Answer identified James Dwyer, Director, Technology Center 2100. However, the Technology Center Director did not sign the Examiner's Answer.

Applicants note, however, that the Supervisory Patent Examiner did sign the Examiner's Answer.

Accordingly, Applicants respectfully request that the Examiner confirm that the new ground of rejection has been properly approved by the Technology Center (TC) Director or designee, in compliance with 37 C.F.R. § 41.39(a)(2) (see also M.P.E.P. § 1207.03).

III. CONCLUSION

In view of the foregoing, Applicants submit that claims 1, 5-9, and 11-36, all the claims presently pending in the application, are patentably distinct over the prior art of record and are in condition for allowance. The Examiner is respectfully requested to pass the above application to issue at the earliest possible time.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

The Commissioner is hereby authorized to charge any deficiency in fees or to credit any overpayment in fees to Assignee's Deposit Account No. 50-0510.

Respectfully Submitted,

Date: January 16, 2007

John J. Dresch, Esq.
Registration No. 46,672

Sean M. McGinn, Esq.
Registration No. 34,386

**MCGINN INTELLECTUAL PROPERTY
LAW GROUP, PLLC**
8321 Old Courthouse Road, Suite 200
Vienna, Virginia 22182-3817
(703) 761-4100
Customer No. 21254

CERTIFICATE OF TRANSMISSION

I certify that I transmitted via USPTO Electronic Filing System (EFS) the enclosed Amendment under 37 C.F.R. § 1.111 to Examiner Christian A. La Forgia, Art Unit 2131, on January 16, 2007.

John J. Dresch, Esq.
Registration No. 46,672
Sean M. McGinn, Esq.
Registration No. 34,386